Agosto de 2015

MANUAL DE USUARIO

MESA DE SERVICIO SGSI

La aplicación Web Mesa de Servicio SGSI es un sistema que utilizan los usuarios de los servicios críticos que brinda el Ministerio de Hacienda para reportar los eventos e incidentes de seguridad de la información

DINAFI
Ministerio de Hacienda
Agosto de 2015

Contenido

INTRODUCCION 3

DEFINICIONES 3

I. INGRESO A LA APLICACION 4

II. USO DE LA APLICACIÓN 7

1. CARACTERISTICAS GENERALES 7

A. BARRA DE USUARIO 7

B. BARRA DE MENÚ 7

2. ENVIO DE SOLICITUD 8

A. ¿A quien afecta? (se refiere al usuario) 10

B. ¿Cuál es el problema?. 10

C. Categorías. 11

D. Descripción detallada del incidente 11

E. Agregar Documento 12

F. Remover documento seleccionado 15

G. Buscar en la base de conocimientos 15

III. SEGUIMIENTO A SOLICITUD PRESENTADA. 199

A. Tareas Recientes 19

B. Mi reporte de tareas 20

C. Abrir caso 21

D. Agregar un comentario a un incidente 21

E. Visualizar comentario en un incidente 22

INTRODUCCION

La aplicación web mesa de servicio SGSI es un sistema que se utiliza para reportar eventos e incidentes de seguridad de la información, presentados por los usuarios que hacen uso de los sistemas de información de la institución, permitiendo llevar el registro y seguimiento a los eventos e incidentes reportados. Adicionalmente nos permitirá contar con una base de conocimientos para facilitar el análisis, aprendizaje y prevención de los incidentes de seguridad.

DEFINICIONES

Evento de seguridad de la información: Es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en los controles (salvaguarda o medida de seguridad) o una situación previamente desconocida que puede ser relevante para la seguridad de la información (afecta la confidencialidad, integridad o disponibilidad de la información o los sistemas).

Incidente de seguridad de la información: Es cualquier actividad que perjudique o represente una amenaza grave para la totalidad o parte de los equipos informáticos o en la red de la institución, de tal manera que haya provocado la falta del servicio, la degradación considerable del funcionamiento de los sistemas, cambios no autorizados en el hardware, firmware, software o datos que afecten la seguridad de la información o que expongan de forma no autorizada información confidencial y reservada de la institución, un desastre natural que destruya el acceso o el control de estos recursos. Para propósitos de estos lineamientos únicamente se consideraran los relacionados con: Denegación de servicio, Phishing, código malicioso y acceso no autorizado.

En este documento se presenta una breve explicación de cada una de sus funciones, iniciando con el ingreso a esta.

I. INGRESO A LA APLICACIÓN

Para ingresar a esta aplicación (mesa de servicio SGSI) es necesario iniciar la sesión desde un browser o navegador, para este manual usaremos Internet Explorer, el cual accedemos dando clic en inicio/ todos los programas/ y luego Internet Explorer, como se muestra en la figura:

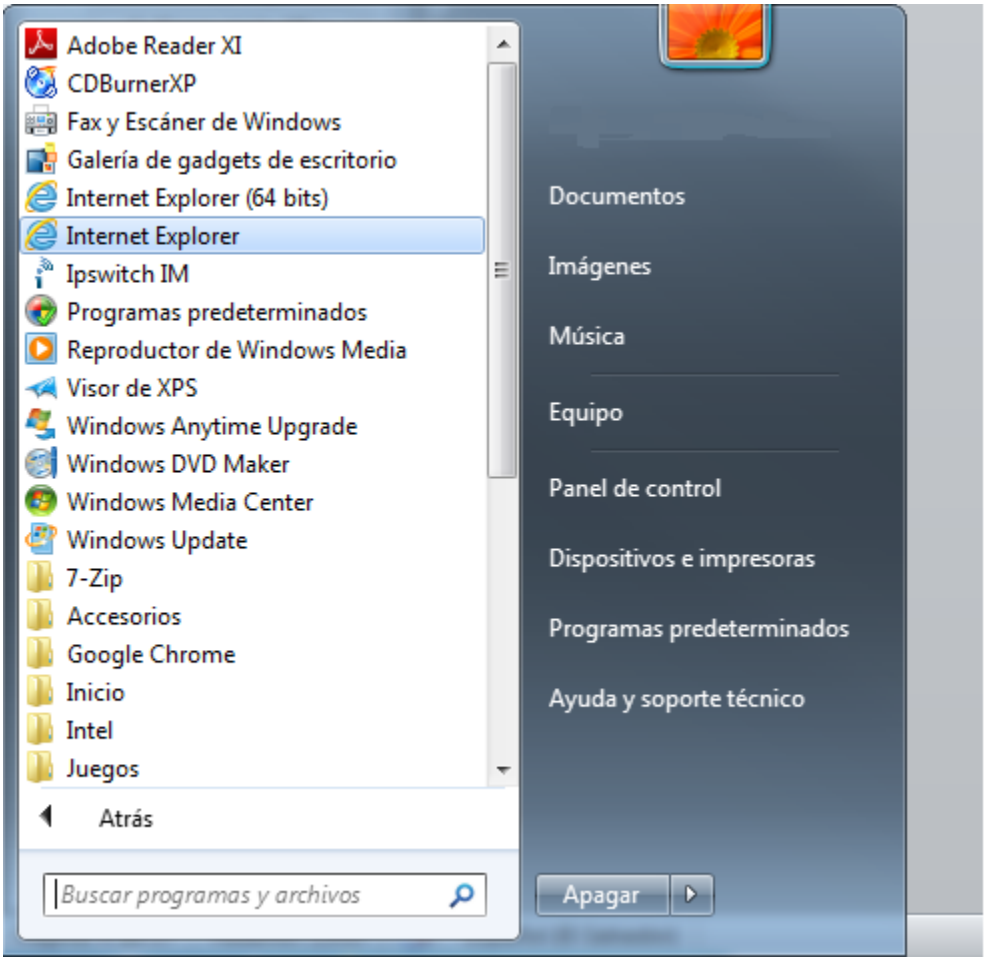

Figura 1: Selección de navegador

Luego que el navegador nos muestre su pantalla de inicio, puede acceder de dos maneras:

1. Ir a la barra de dirección e ingresamos la siguiente URL http://incidentessgsi/ProcessManager/. Veremos lo siguiente:

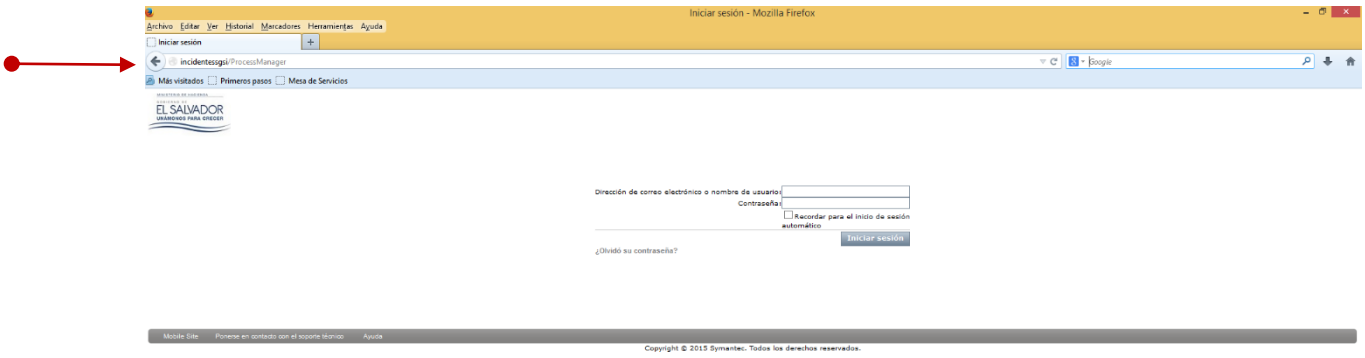
Iniciar sesión - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Iniciar sesión
incidentessgsi/ProcessManager
Más visitados Primeros pasos Mesa de Servicios
EL SALVADOR
Dirección de correo electrónico o nombre de usuario
Contraseña
Recordar para el inicio de sesión automático
Iniciar sesión
¿Olvidó su contraseña?
Copyright © 2015 Symantec. Todos los derechos reservados.

Figura 2: Ingresando URL

2. Ir a la dirección del SGSI () y dar clic al enlace de la Mesa de Servicios SGSI, como se muestra a continuación:

Día 25 del Mes 08 del año 2015
Servicios
MINISTERIO DE HACIENDA
GOBIERNO DE EL SALVADOR
Aduanas
Compras
Bienvenido :
Logout
Buscar
Mesa de Servicios SGSI
SGSI
SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION
NOTA
* Si después de que usted cambió su contraseña, solicitó al administrador que le resetee su contraseña, o se cambió de unidad organizativa (Dirección, departamento, sección, otro); la información que le muestra el Portal SGSI está desactualizada, intente borrar las cookies y archivos temporales de Internet Explorer. Si esto no resuelve el problema, informe al Encargado de Seguridad de la Información de su dependencia.
* Para los usuarios que utilizan SAFII y/o SAFIC, la contraseña será la misma para acceder al portal del SGSI.
* Se requiere tener como mínimo la versión 7 de acrobat reader para poder visualizar los documentos en formato PDF.
* link para poder descargar acrobat reader:
http://get.adobe.com/es/reader/
PASOS PARA OBTENER ACCESO AL PORTAL
CAMBIO DE CLAVE
Este portal contiene los documentos del SGSI. Es requisito poseer un usuario y contraseña autorizados para ingresar a estos documentos. Si necesita cambiar la contraseña de acceso a Portal, Favor dar clic en la imagen.
1 - DOCUMENTOS COMPARTIDOS DEL SGSI
7 - DINAFI
DIRECCION NACIONAL DE ADMINISTRACION FINANCIERA E INNOVACION
Enlaces de Interes
Estándares, Buenas Prácticas, Revistas...
Los 8 Puntos...
Cuentas y Contraseñas 1
Cuentas y Contraseñas 2
Control de Accesos 1
Correo Electrónico 1
Ver más...
New Tab
Boletin de Seguridad
Bos 1 Phishing y Estafas en el Correo Electrónico
Bos 2 Cómo identificar un correo falso
Bos 3 Correo Ebola y Verificación de Antivirus
Términos de Seguridad
Glosario
Quienes somos
Encargados de Seguridad
Contáctenos
seguridad@mh.gob.sv
© 2009 Ministerio de Hacienda todos los derechos reservados
Conmutador: 2244-3000 - Boulevar "Los Héroes" No. 1231, San Salvador, El Salvador , C.A.
Resolución mínima 800 X 600
Este sitio se ve mejor con Internet Explorer 7.0, Mozilla Firefox 2.0, ó superior

Figura 3: Mesa de Servicios SGSI en el Portal

Para ambas formas de acceder se presentará la siguiente pantalla de Ingreso:

Ingreso con correo electrónico institucional

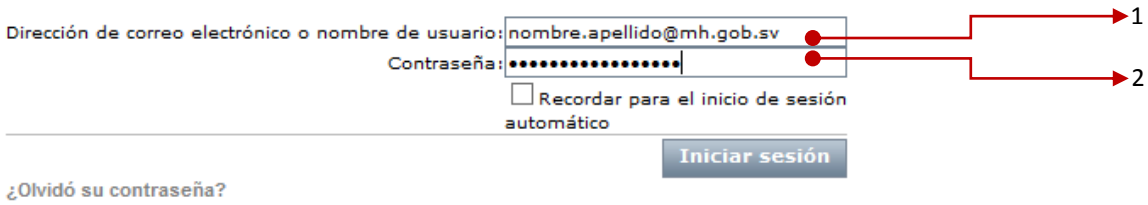

Figura 4: Pantalla de validación de ingreso en el sistema

La figura anterior nos muestra una pantalla de validación de usuario en la que proporcionamos nuestros datos para ingresar a la aplicación.

1. El campo “número uno”, nos solicita la dirección de correo electrónico institucional o nombre de usuario. Colocamos la dirección de correo electrónico, por ejemplo: nombre.usuario@mh.gob.sv

2. En el campo “número dos” debe ingresar su contraseña, que es la misma que utiliza para ingresar a su computadora.

Si los datos “Usuario” y “Contraseña” son correctos veremos la siguiente pantalla

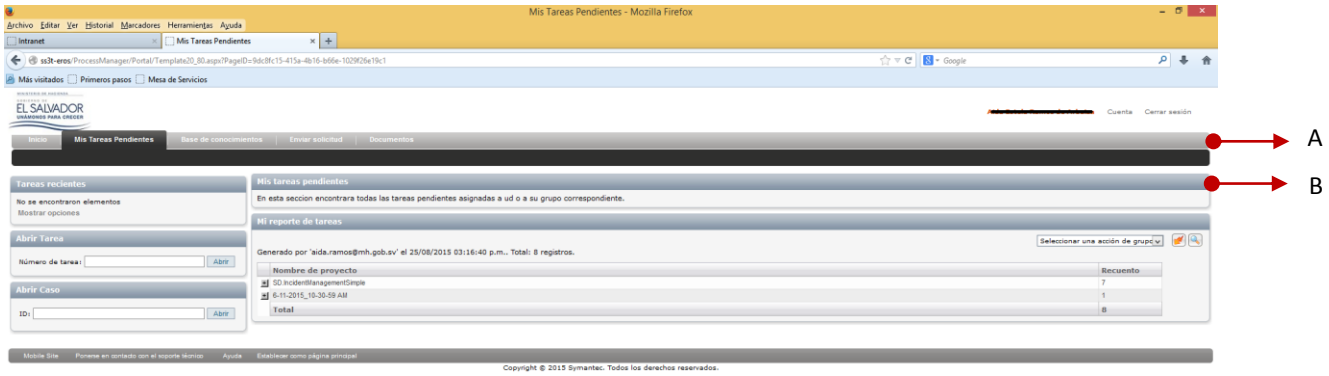

Figura 5: Pantalla de inicio del sistema

En esta pantalla tenemos acceso a las áreas de:

A) Barra de Usuario
B) Barra de Menú

Que se utilizan para navegar en las diferentes opciones que nos brinda la aplicación según se detalla a continuación.

II. USO DE LA APLICACIÓN

1. CARACTERISTICAS GENERALES

Se detalla a continuación el contenido en cada una de las opciones:

A) Barra de Usuario
B) Barra de Menú

A. BARRA DE USUARIO

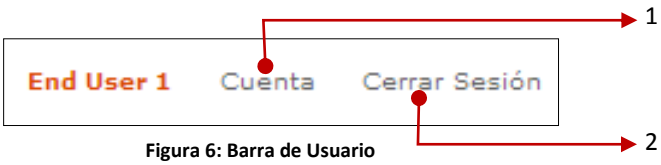

Figura 6: Barra de Usuario

Una vez se logra el ingreso aparecerá el nombre del usuario, ejemplo: aida.ramos (en el espacio que se muestra en rojo en la barra), así como las opciones de menú "Cuenta" y "Cerrar Sesión" que nos serán de mucha ayuda en el uso de la herramienta:

1. Cuenta (en esta opción se puede visualizar Información de la cuenta tal como el grupo(s) al que pertenece, número de teléfono, correo electrónico, dirección)
2. Cerrar Sesión (opción que se utiliza para finalizar o cerrar el sistema)

B. BARRA DE MENÚ

Figura 7: Barra de menú

En esta barra podemos ver las diferentes opciones que nos permiten navegar por la aplicación y realizar las tareas que podamos requerir.

1. **Inicial** (Muestra la página principal del Sistema de Mesa de Servicio).
2. **Mis Tareas Pendientes** (Muestra los requerimientos que le han sido asignados hasta el momento)
3. **Base de conocimientos** (En esta opción se visualizan las soluciones aplicadas a los incidentes de seguridad de la información de las Direcciones o Dependencias con el propósito que puedan

ser utilizadas a la solución de incidentes similares, facilitando el análisis, aprendizaje y prevención de los incidentes de seguridad de la información).

4. **Enviar solicitud** (Este botón nos lleva a la página donde realizaremos el envío de la solicitud para la atención de un evento de seguridad de la información)

C. ENVIO DE SOLICITUD

Al seleccionar en la barra de menú *Enviar solicitud* encontrará la opción para la creación de un nuevo evento de seguridad de la información:

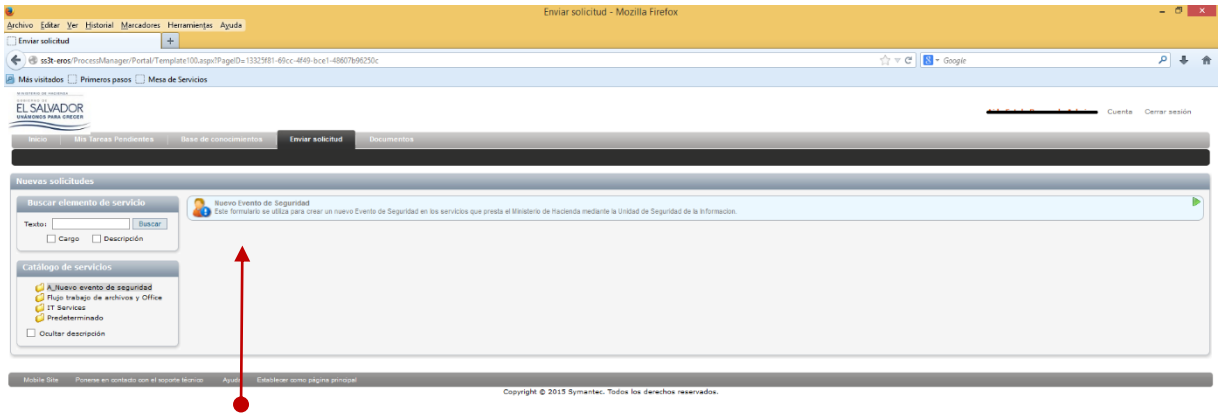
Enviar solicitud - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Enviar solicitud
Más visitados Primeros pasos Mesa de Servicios
EL SALVADOR
Cuenta Cerrar sesión
Inicio Mis Tareas Pendientes Base de conocimientos Enviar solicitud Documentos
Nuevas solicitudes
Buscar elemento de servicio
Texto: Buscar
Cargo Descripción
Catálogo de servicios
A_Nuevo evento de seguridad
Flujo trabajo de archivos y Office
IT Services
Predeterminado
Ocultar descripción
Nuevo Evento de Seguridad
Este formulario se utiliza para crear un nuevo Evento de Seguridad en los servicios que presta el Ministerio de Hacienda mediante la Unidad de Seguridad de la Información.
Mobile Site Ponerse en contacto con el soporte técnico Ayuda Establecer como página principal
Copyright © 2015 Symantec. Todos los derechos reservados.

Figura 8: Flujo de trabajo creación de evento de seguridad

Al seleccionar la opción *Nuevo evento de seguridad*, se abrirá el formulario presentado a continuación.

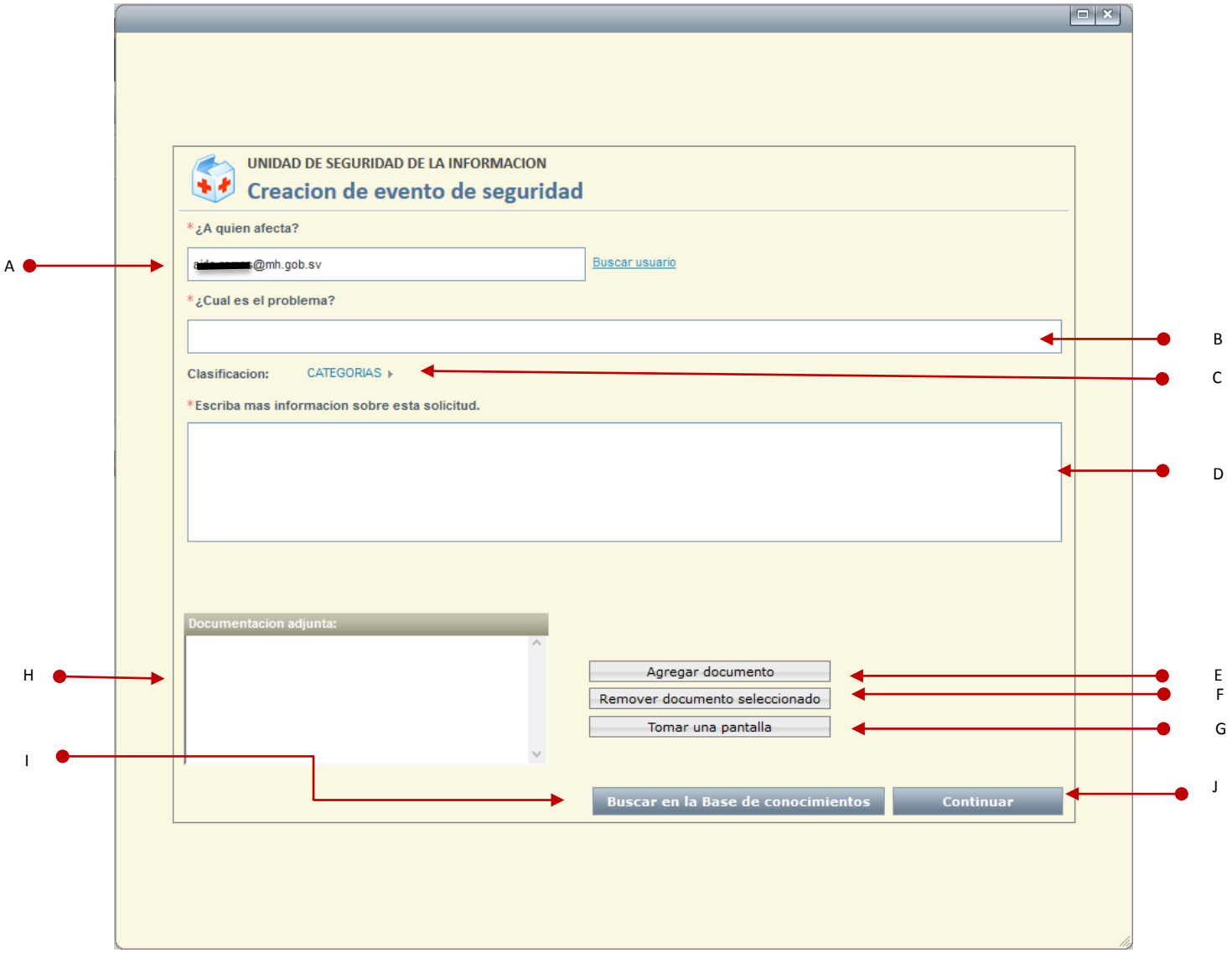

Figura 9: Creación de evento de seguridad

Esta opción del formulario contiene los campos siguientes:

A)*¿A quién afecta?
B)*¿Cuál es el problema?
C)*Categorías
D)*Detalle de lo que pueda ayudar a resolver este inconveniente
E) Agregar documento
F) Remover documento seleccionado
G) Tomar una pantalla
H) Documentación adjunta
I) Buscar en la Base de Conocimientos
J) Continuar

Nota: Los campos que contengan el asterisco rojo (*) son obligatorios. Si alguno de estos campos no es llenado la solicitud no será enviada.

A) ¿A quién afecta este evento?

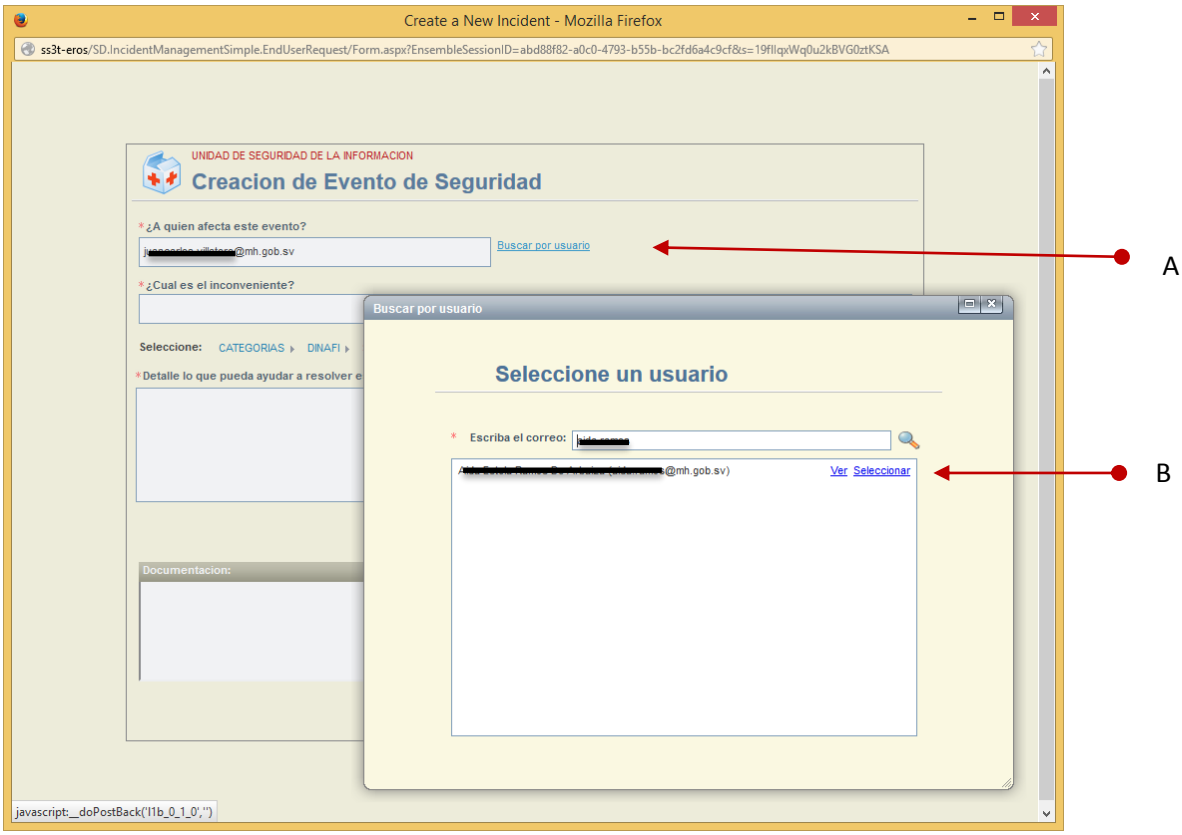

Figura 10: Sección de selección de usuario afectado

Se debe seleccionar el usuario que ha sido afectado por el evento de seguridad o el responsable de reportarlo(A). Puede realizar una búsqueda (B) escribiendo la dirección de correo institucional y seleccionar de la lista.

B) ¿Cuál es el problema?

UNIDAD DE SEGURIDAD DE LA INFORMACION
Creacion de evento de seguridad
*¿A quien afecta?
Buscar usuario
*¿Cual es el problema?
El Sistema XXXX no ha funcionado durante 2 horas

Figura 11: Sección donde se escribe cuál es el problema

Debe escribir el título o enunciado del evento presentado, el cual debe estar relacionado con el servicio que se ha visto interrumpido, por ejemplo: **El Sistema XXXX no ha funcionado durante 2 horas.**

C) Categorías

Figura 12: Sección de selección de categoría

Se debe seleccionar la categoría de la solicitud. La búsqueda se realiza por selección:

Se elige primero la Dirección o Dependencia afectada por el evento de seguridad de la información, en el segundo nivel se elige "Seguridad de la Información" y para el usuario final debe llegar hasta el nivel "EVENTO DE SEGURIDAD", ejemplo: **DINAFI/SEGURIDAD DE LA INFORMACION/EVENTO DE SEGURIDAD**

D) Detalle lo que pueda ayudar a resolver este inconveniente

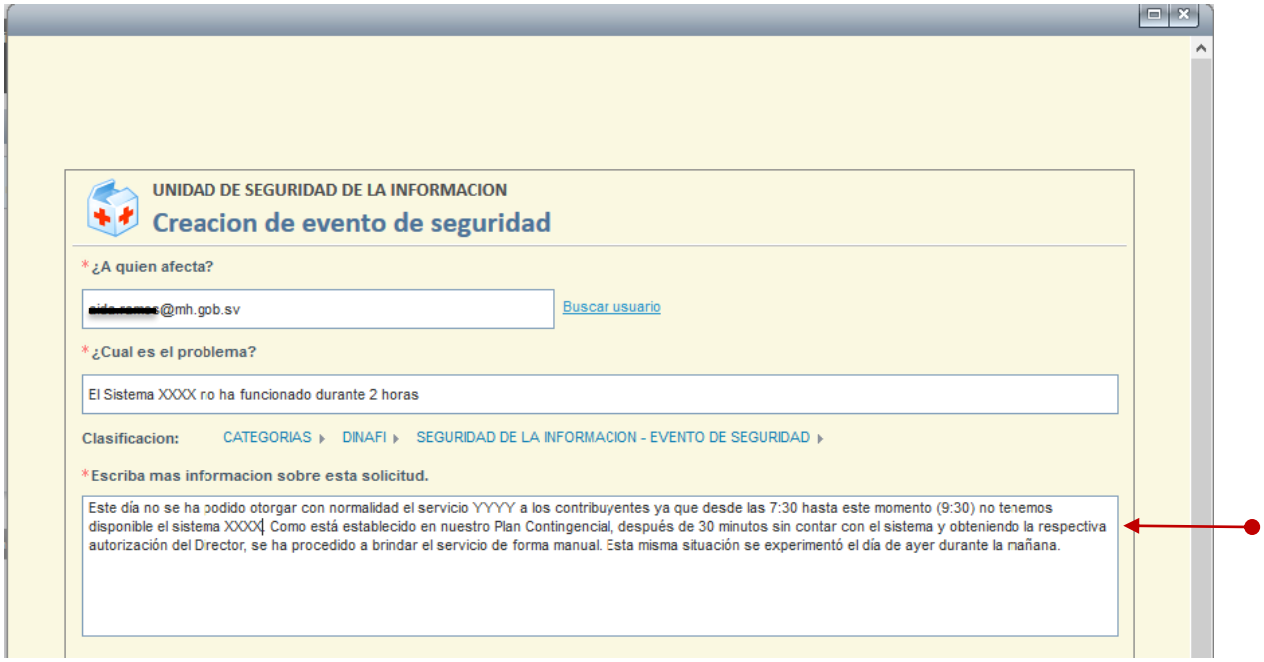
UNIDAD DE SEGURIDAD DE LA INFORMACION
Creacion de evento de seguridad
*¿A quien afecta?
[redacted]@mh.gob.sv
Buscar usuario
*¿Cual es el problema?
El Sistema XXXX no ha funcionado durante 2 horas
Clasificacion:
CATEGORIAS
DINAFI
SEGURIDAD DE LA INFORMACION - EVENTO DE SEGURIDAD
*Escriba mas informacion sobre esta solicitud.
Este día no se ha podido otorgar con normalidad el servicio YYYY a los contribuyentes ya que desde las 7:30 hasta este momento (9:30) no tenemos disponible el sistema XXXX. Como está establecido en nuestro Plan Contingencial, después de 30 minutos sin contar con el sistema y obteniendo la respectiva autorización del Drector, se ha procedido a brindar el servicio de forma manual. Esta misma situación se experimentó el día de ayer durante la mañana.

Figura 13: Sección para agregar el detalle del problema a resolver

Es un área de texto en la cual debe describirse detalladamente el evento de seguridad de la información, los detalles que ayuden al Encargado de Seguridad de su Dirección o Dependencia a ubicarse lo mejor posible en lo ocurrido y orientarlo para buscar alternativas de solución que permitan resolver el evento de seguridad o determinar si éste debe escalarse a la categoría de "INCIDENTE DE SEGURIDAD".

Nota: Es importante tener el cuidado de no incluir en este texto información clasificada como Reservada o Confidencial, o cualquier otra que pudiera afectar la seguridad de la información, como por ejemplo: contraseñas, imágenes de documentos de identificación personal, números de teléfonos y domicilio personales.

E) Agregar Documento

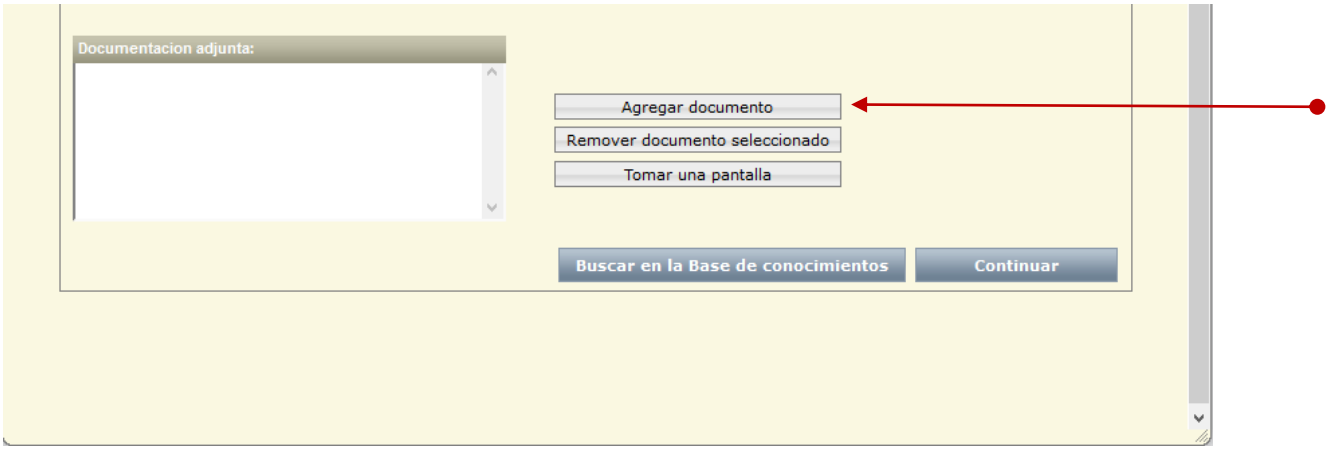

Figura 14: Sección para adjuntar documento

Si es necesario incluir en la solicitud algún archivo que refuerce la explicación o análisis del caso, en la sección *Agregar documento* puede hacerlo de la siguiente manera:

Haga clic en el botón *Agregar documento*. Aparecerá una pantalla en la cual deberá seleccionar el archivo:

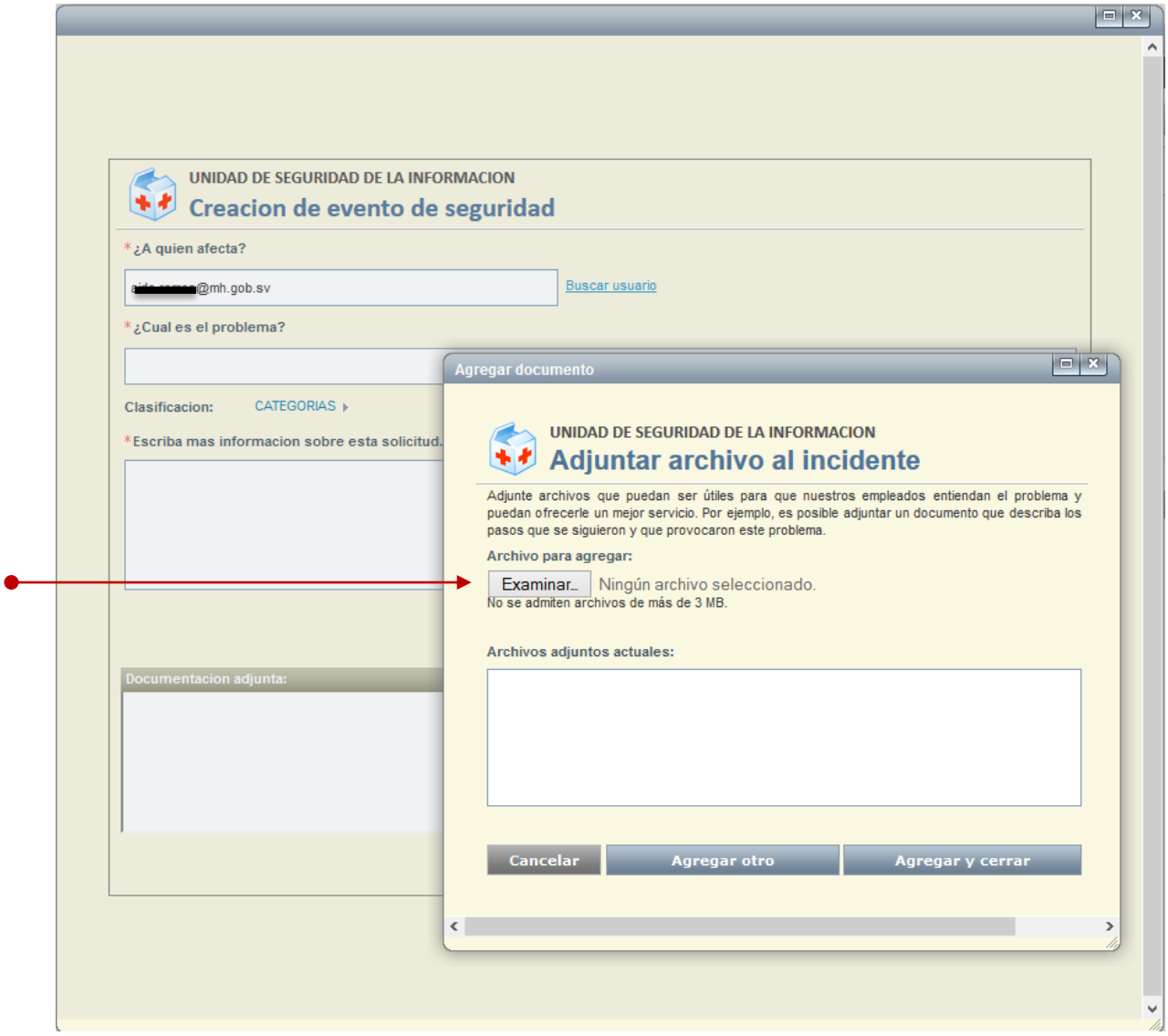
UNIDAD DE SEGURIDAD DE LA INFORMACION
Creacion de evento de seguridad
*¿A quien afecta?
[redacted]@mh.gob.sv
Buscar usuario
*¿Cual es el problema?
Clasificacion:
CATEGORIAS
*Escriba mas informacion sobre esta solicitud.
Documentacion adjunta:
Agregar documento
UNIDAD DE SEGURIDAD DE LA INFORMACION
Adjuntar archivo al incidente
Adjunte archivos que puedan ser útiles para que nuestros empleados entiendan el problema y puedan ofrecerle un mejor servicio. Por ejemplo, es posible adjuntar un documento que describa los pasos que se siguieron y que provocaron este problema.
Archivo para agregar:
Examinar...
Ningún archivo seleccionado.
No se admiten archivos de más de 3 MB.
Archivos adjuntos actuales:
Cancelar
Agregar otro
Agregar y cerrar

Figura 15: Formulario para adjuntar documentos

Oprima el botón *Examinar* para elegir de su lista de archivos y oprima el botón *Abrir* para seleccionar el que va a adjuntar a la solicitud:

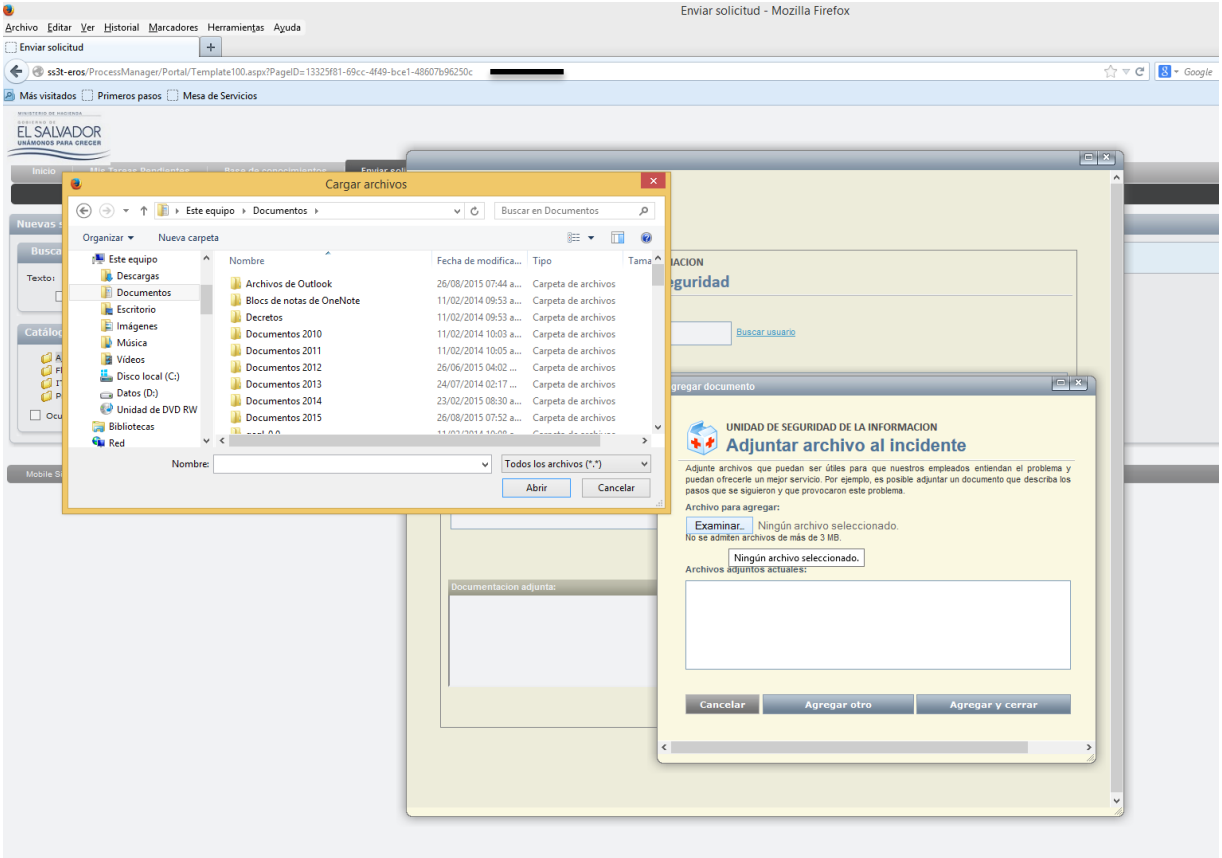

Figura 16: Adjuntar archivos

Una vez identificado el documento, selecciónelo y oprima el botón *Agregar y cerrar*, o si desea seguir agregando archivos oprima el botón *Agregar otro* hasta finalizar.

Nota. La capacidad de los archivos no debe exceder a 3 Mb.

En el cuadro Documentación se podrán visualizar los archivos que han sido adjuntados a la solicitud (A)

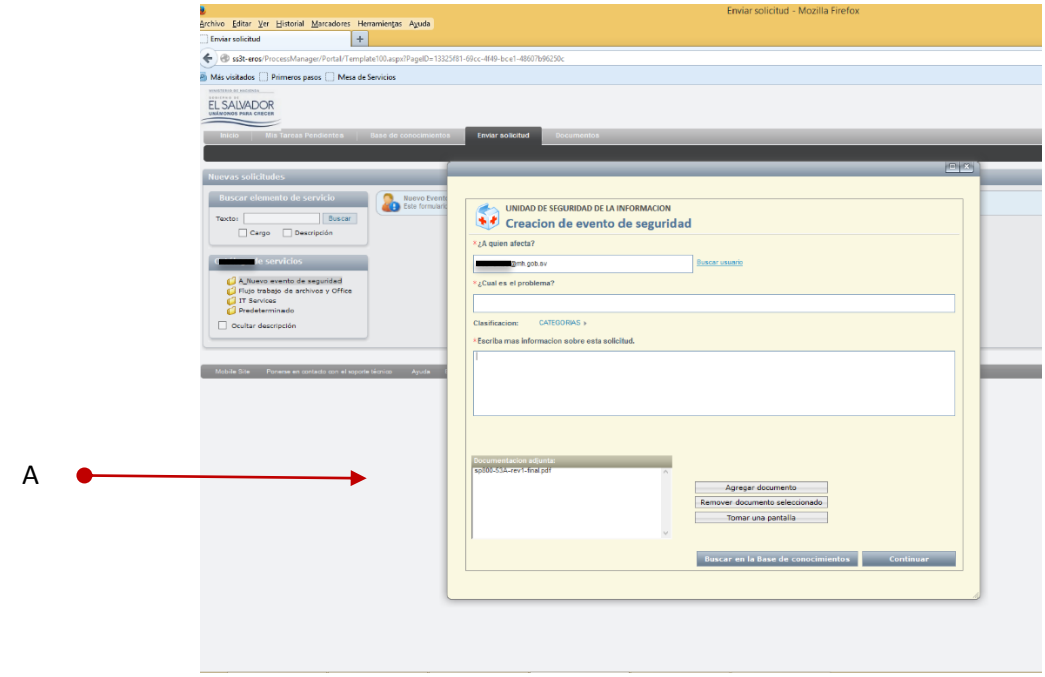

Figura 17: Documentos adjuntados a la solicitud

F) Remover documento seleccionado

Si desea eliminar el documento o los documentos agregados a la solicitud, haga clic sobre el (los) nombre del documento (s) (A) y presione el botón "*Remover documento seleccionado*" (B):

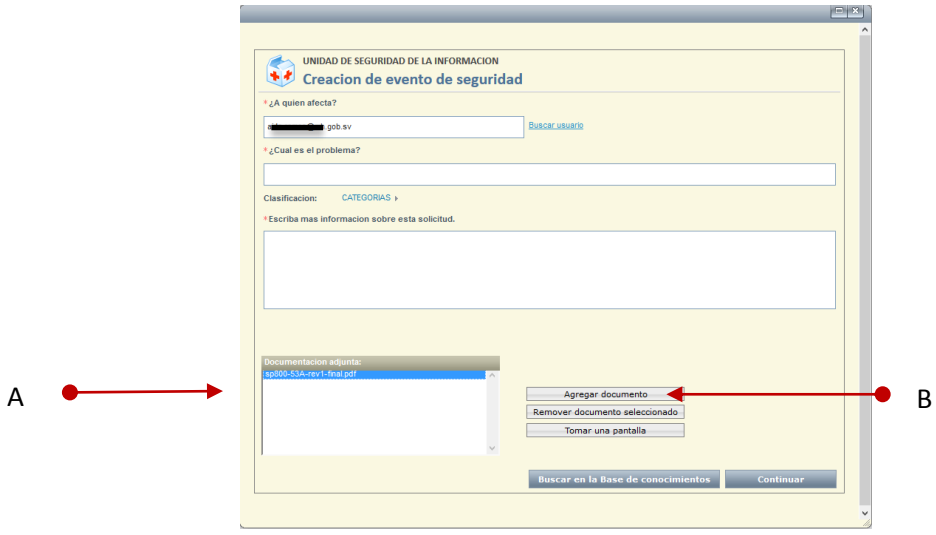

Figura 18: Remover documento seleccionado

G) Buscar en la base de conocimientos

Una base de conocimientos no es más que una base de datos para la gestión del conocimiento, y en este caso es posible que exista información de la resolución de eventos o incidentes de seguridad de

la información anteriores con la cual se le pueda dar solución a su solicitud, es por eso que antes de enviar la solicitud se recomienda buscar en la base de conocimientos.

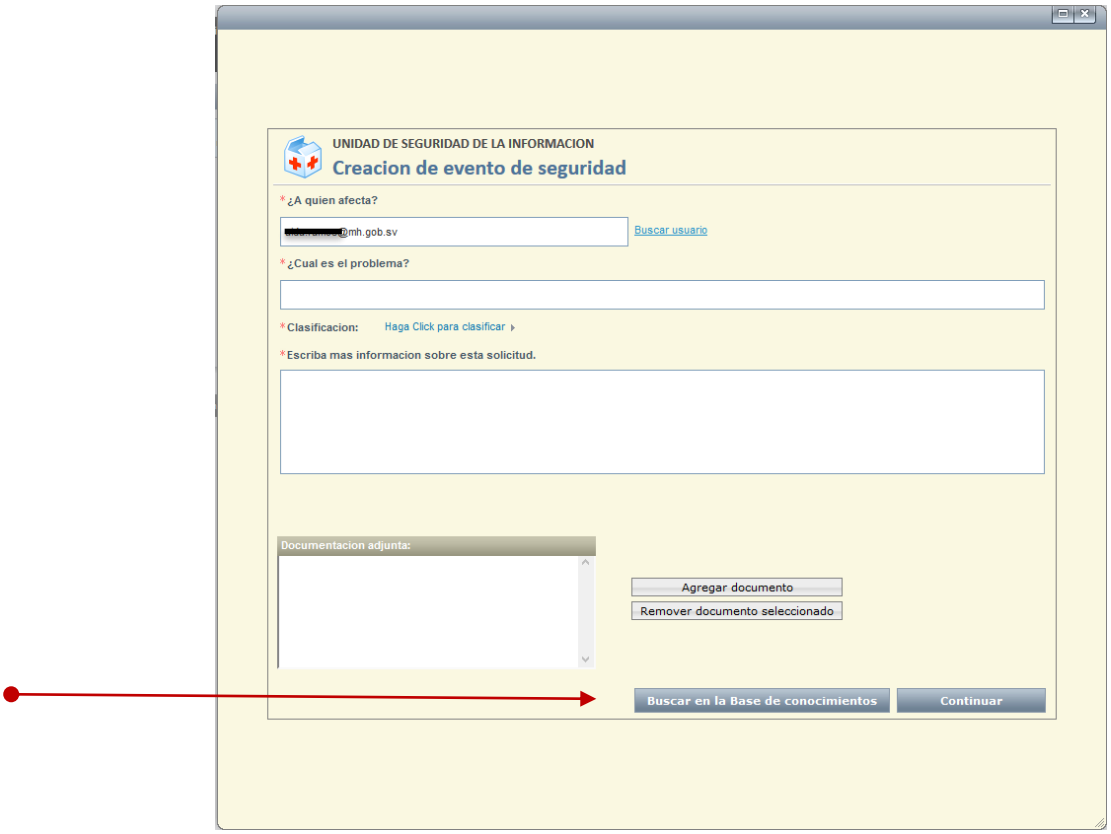

Figura 19: Gestión de base de conocimientos

Al dar clic sobre el botón *Buscar en la base de conocimientos* aparecerá la siguiente ventana de búsqueda de información:

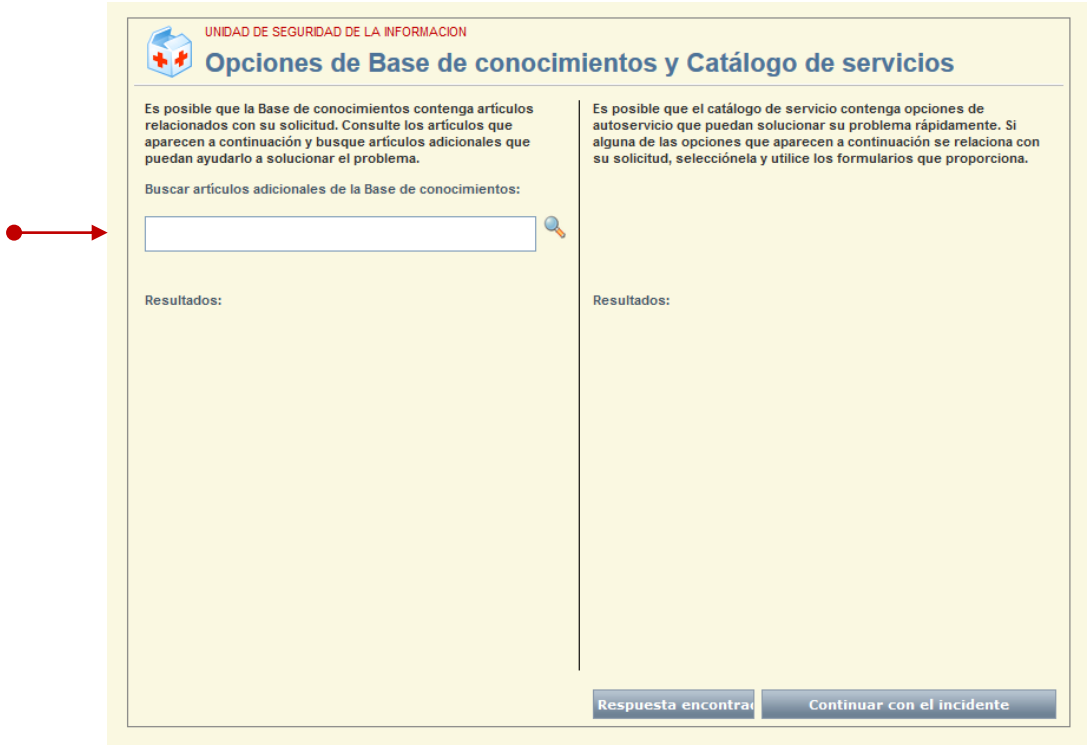
UNIDAD DE SEGURIDAD DE LA INFORMACION
Opciones de Base de conocimientos y Catálogo de servicios
Es posible que la Base de conocimientos contenga artículos relacionados con su solicitud. Consulte los artículos que aparecen a continuación y busque artículos adicionales que puedan ayudarlo a solucionar el problema.
Buscar artículos adicionales de la Base de conocimientos:
Resultados:
Es posible que el catálogo de servicio contenga opciones de autoservicio que puedan solucionar su problema rápidamente. Si alguna de las opciones que aparecen a continuación se relaciona con su solicitud, selecciónela y utilice los formularios que proporciona.
Resultados:
Respuesta encontrad
Continuar con el incidente

Figura 20: Búsqueda en base de conocimientos

Escriba una palabra o una frase relacionada con la información que necesita encontrar y de clic en la figura colocada a la derecha de la caja de texto.

Si la información fue encontrada, le mostrará los resultados y deberá dar clic en el botón *Respuesta encontrada*, de lo contrario seleccione el botón *Continuar con el incidente*.

Si seleccionó el botón *Continuar con el incidente* se mostrará la siguiente pantalla:

UNIDAD DE SEGURIDAD DE LA INFORMACION
Resumen de la solicitud
Datos
Usuario afectado:
Nombre de incidente: Caida en el sistema
Ubicacion: SEDE/Direccion DINAFI/U. de Seguridad de la Informacion
Departmento: SEDE/Direccion DINAFI/U. de Seguridad de la Informacion
Descripcion:
Este día se han presentado tres caidas en el sistema XXX, cada una con una duración de 2 horas aproximadamente, lo que ha provocado falta de servicio de recepción de declaraciones de mercancias en todas las aduanas de El Salvador....
Documentacion adjunta:
TDRs 2016_monitoreo ambiental.docx
Editar
Enviar

Figura 21: Resumen de la solicitud

En la pantalla *Resumen de la solicitud* usted podrá realizar la revisión final y corregir la información registrada oprimiendo el botón *Editar* o *Enviar* si la información es correcta y está completa. Luego de hacer esto, el sistema nos proporcionará el número de requerimiento:

UNIDAD DE SEGURIDAD DE LA INFORMACION
¡Gracias!
Nueva Id. de proceso del incidente: IM-000032
Su solicitud ha sido enviada exitosamente.
Para consultar el estado de las solicitudes que realizó, inicie sesión en ServiceDesk y vaya a la ficha "Inicio". ServiceDesk está disponible en http://ss3t-eros:80/ProcessManager.
Iniciar una nueva solicitud
Confirmar y cerrar

Figura 22: Requerimiento Creado

Si usted desea ingresar otra solicitud oprima el botón *Iniciar una nueva solicitud* y repita el proceso descrito en los literales A al L, de lo contrario oprima el botón *Confirmar y cerrar* y automáticamente recibirá por medio de correo electrónico de que su solicitud ha sido creada.

III. SEGUIMIENTO A SOLICITUD PRESENTADA

Si necesita realizar seguimiento a las solicitudes ingresadas, en la barra de menú encontrará la opción "*Mis tareas pendientes*":

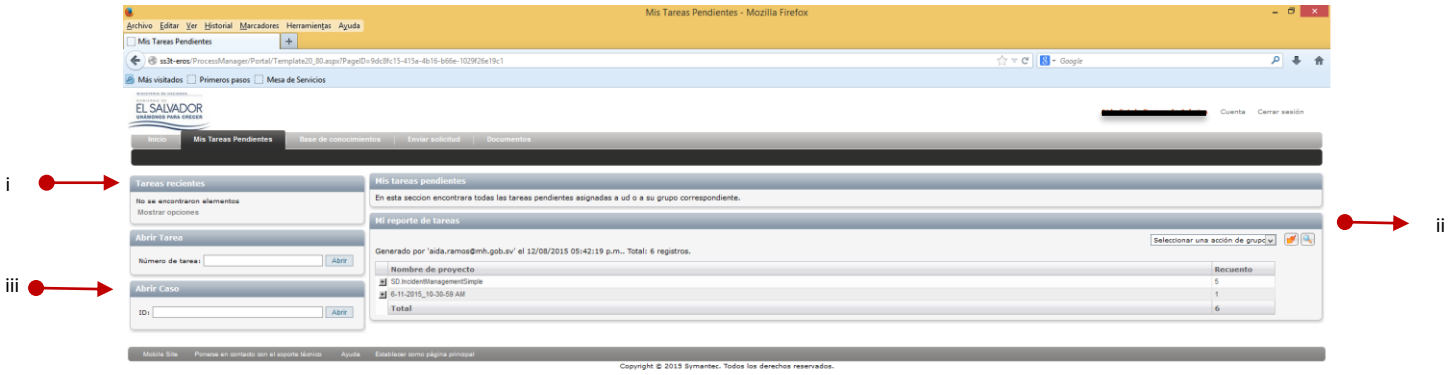

Figura 23: Mis tareas pendientes

Contiene las secciones siguientes:

A. Tareas Recientes. En este recuadro se muestran los incidentes o solicitudes que hubiese presentado a la Mesa de Servicios SGSI.
B. Mi reporte de Tareas. Visor de tareas que muestra las solicitudes atendidas.
C. Abrir Caso. Esta opción se utiliza para buscar solicitudes por número asignado, y deberá escribirlo con el formato siguiente: IM-000001

A. Tareas Recientes

En esta parte de la página se muestra un historial de las solicitudes, base de conocimientos y otros artículos consultados durante la sesión del usuario en el sistema. Al mismo tiempo cuenta con opciones de personalización o búsqueda si es que el usuario ha consultado varios reportes y base de conocimientos:

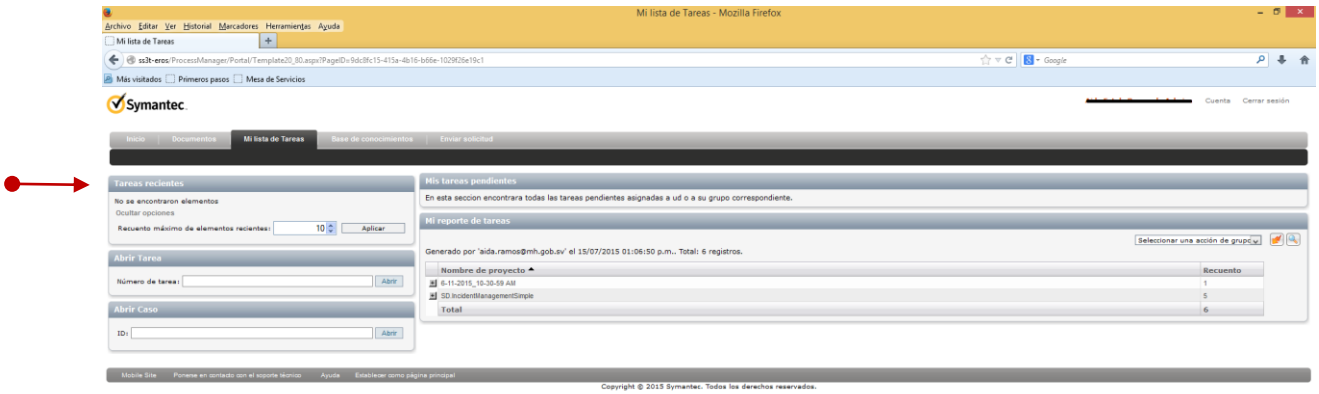

Figura 24: Tareas recientes

B. Mi reporte de tareas

Esta sección presenta una tabla con los incidentes que han sido resueltos y cerrados por el técnico. Para cada uno es necesario que como usuarios demos el visto bueno a la solución que el técnico nos ofrece, para ello debemos seleccionar uno de los informes que aparecen en la tabla, hacer clic en la opción de la tabla que dice *Haga Clic aquí para revisar y cerrar su incidente*.

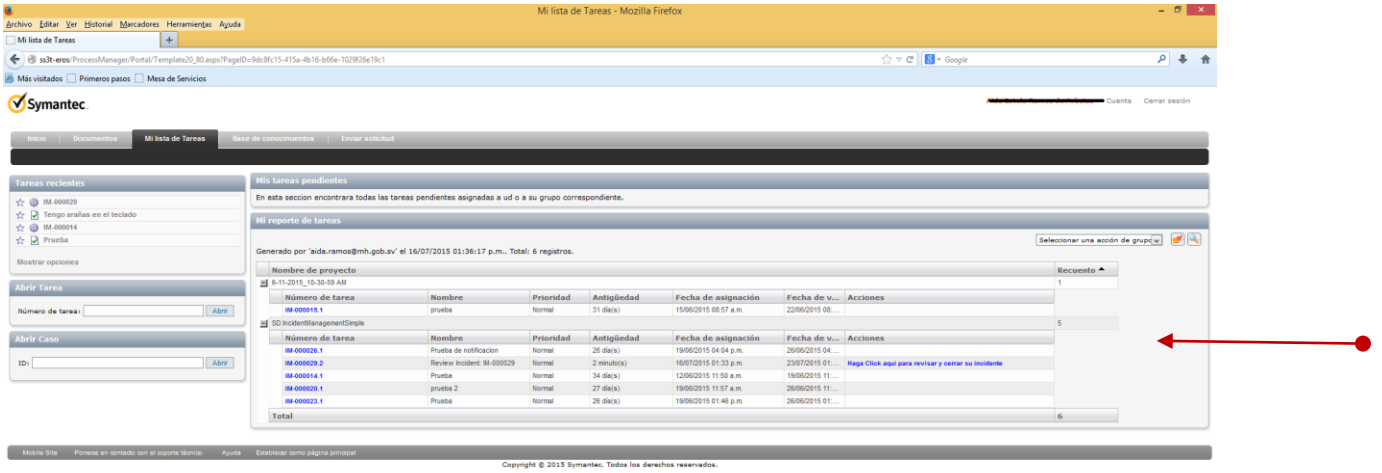
Mi lista de Tareas - Mozilla Firefox
Symantec
Mis tareas pendientes
Mi reporte de tareas
Haga Click aquí para revisar y cerrar su incidente

Figura 25: Visor de Tareas

La pantalla nos mostrará información relacionada con la solución de la solicitud, si consideramos que la resolución brindada por el técnico es satisfactoria, procederemos a cerrar la solicitud con un clic en el botón *Caso resuelto*:

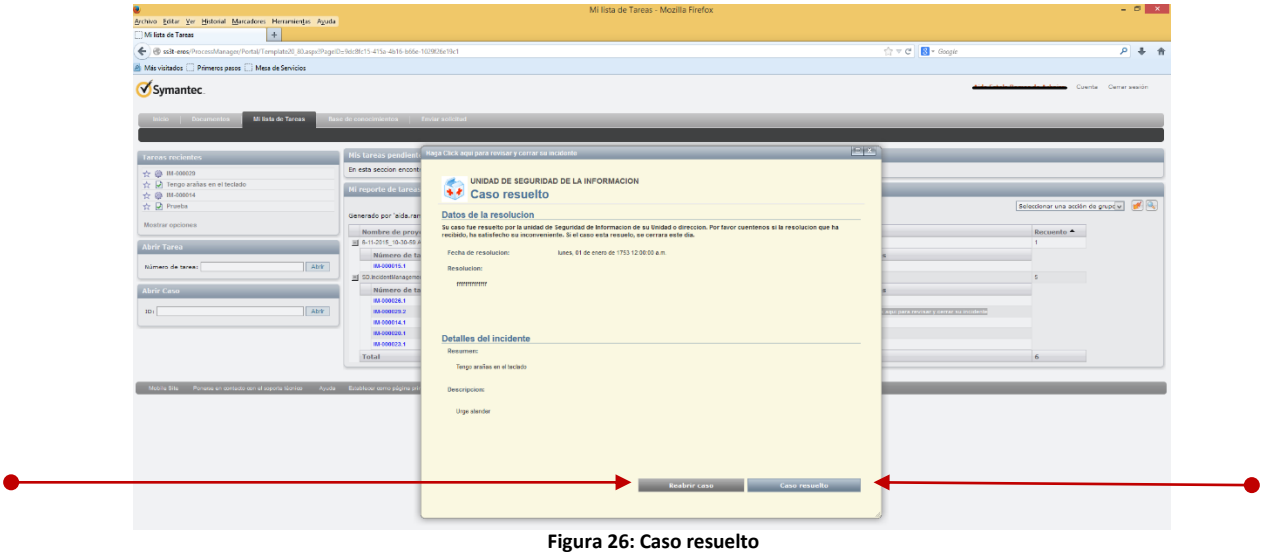

Figura 26: Caso resuelto

Nota. Si no realizamos esta actividad la solicitud se mantendrá en un 90% de realización, por lo que es necesario completarlo con el 10% correspondiente al cierre.

Si el usuario no está satisfecho con la solución decidirá si re-abrir el incidente con un clic en el botón *Reabrir caso*:

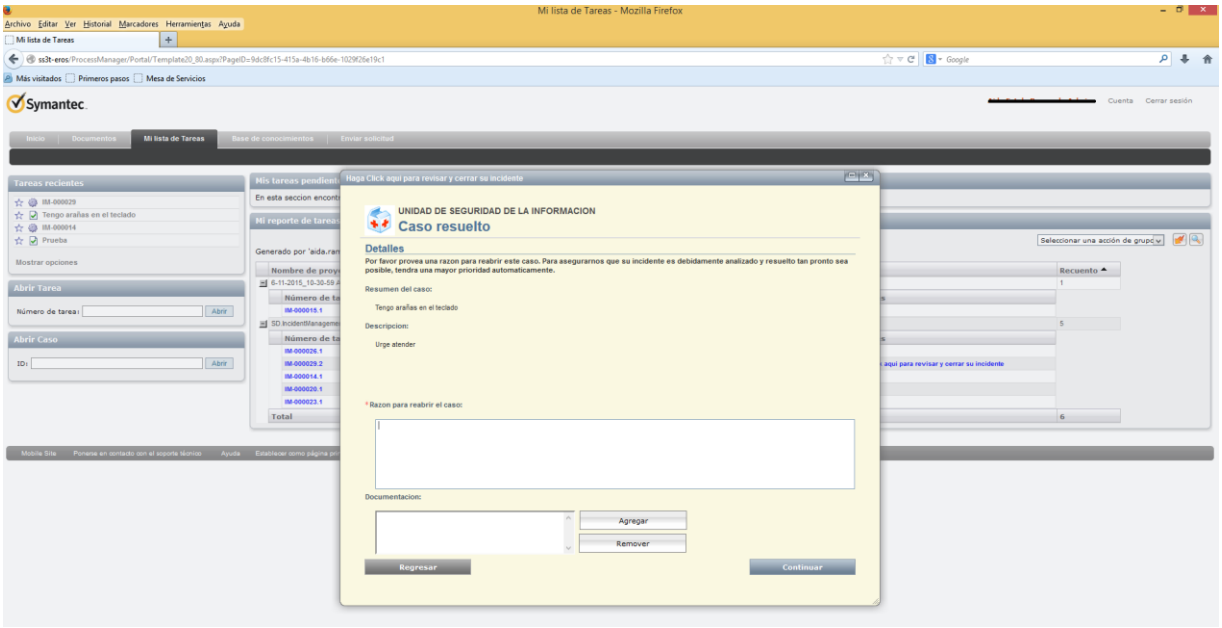
Mi lista de Tareas - Mozilla Firefox
Symantec
Haga Click aqui para revisar y cerrar su incidente
UNIDAD DE SEGURIDAD DE LA INFORMACION
Caso resuelto
Detalles
Por favor provea una razon para reabrir este caso. Para asegurarnos que su incidente es debidamente analizado y resuelto tan pronto sea posible, tendra una mayor prioridad automaticamente.
Resumen del caso:
Tengo arañas en el teclado
Descripcion:
Urge atender
*Razon para reabrir el caso:
Documentacion:
Agregar
Remover
Regresar
Continuar

Figura 27: Reabrir caso

En la sección *Razón para reabrir el caso* deberá describir los motivos por los cuales considera que su solicitud no ha sido resuelta, además podrá adjuntar documentación que justifique su inconformidad haciendo clic en el botón *Agregar Archivo*.

Ahora proceda a dar clic al botón *Continuar* y su solicitud volverá a la lista de tareas asignadas.

C. Abrir Caso

Para la búsqueda de eventos debe ingresar el número de solicitud con su respectiva nomenclatura, de la siguiente forma:

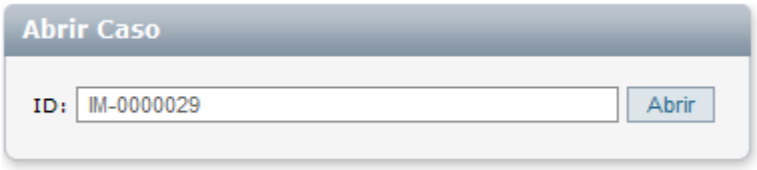

Figura 28: Búsqueda de incidentes

D. Agregar un comentario a un incidente

Únicamente el usuario afectado en el evento de seguridad de la información podrá agregar comentarios a una solicitud y lo hará haciendo clic en la opción *Agregar un comentario:*

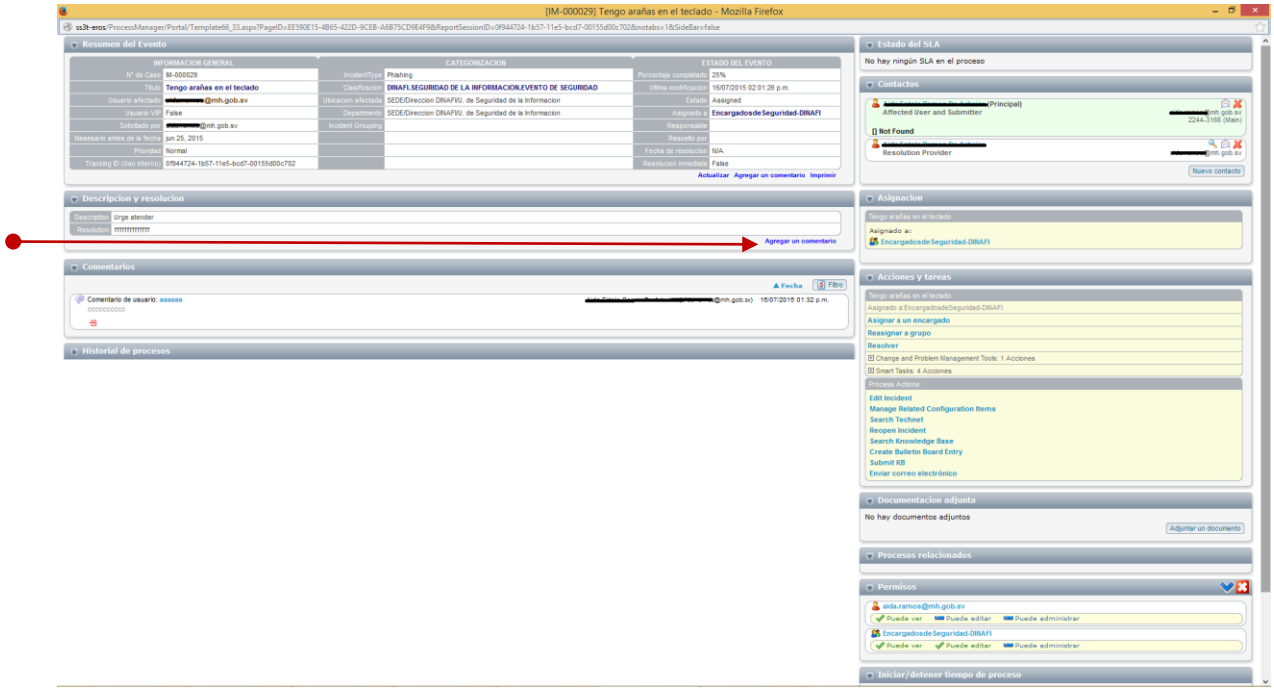

Figura 29: Ventana Agregar comentario

Nos mostrara una ventana donde podremos ingresar el título y el comentario que deseamos agregar a la solicitud, y luego hacemos clic en el botón *Guardar*:

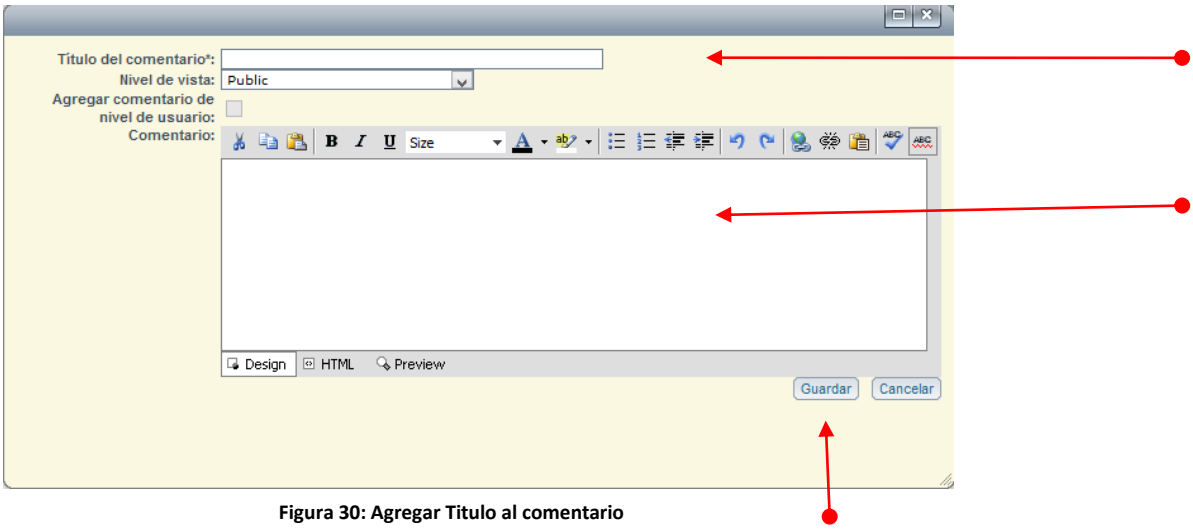

Figura 30: Agregar Titulo al comentario

E. Visualizar comentario en un incidente

Para poder visualizar los comentarios de una solicitud, debemos ingresar y en la opción *historial* muestra los comentarios que han sido adicionados por los técnicos.

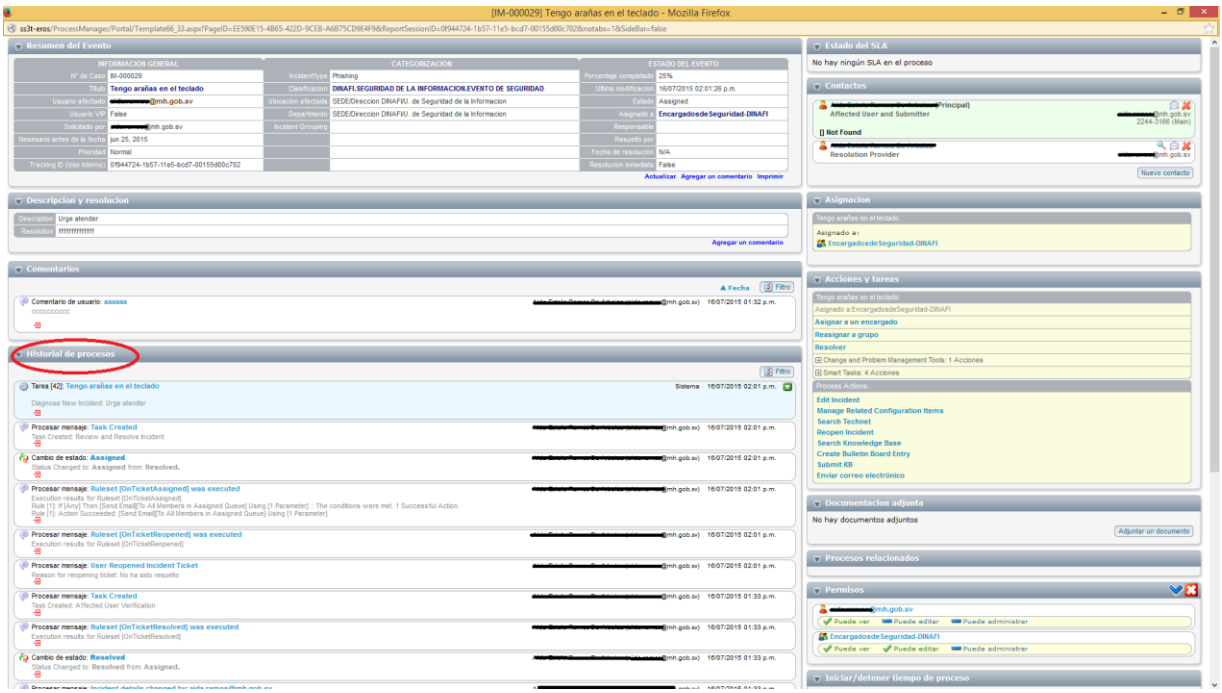

Figura 31: Visualizar el historial de comentarios del evento de seguridad de la información